The opinion in support of the decision being entered today was <u>not</u> written for publication and is <u>not</u> binding precedent of the Board.

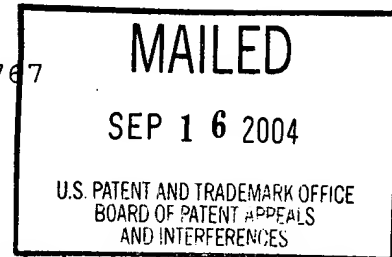<div align="right">Paper No.20</div>

<div align="center">

UNITED STATES PATENT AND TRADEMARK OFFICE

———————

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

———————

Ex parte SARVAR PATEL

———————

Appeal No. 2003-0446
Application No. 09/127,767

———————

ON BRIEF

———————

</div>

Before HAIRSTON, GROSS, and BLANKENSHIP, **Administrative Patent Judges.**

GROSS, **Administrative Patent Judge.**

<div align="center">

DECISION ON APPEAL

</div>

This is a decision on appeal from the examiner's final rejection of claims 1 through 22, which are all of the claims pending in this application.

Appellant's invention relates to a method of authenticating parties communicating with one another to provide a security measure to their communication. Claim 12 is illustrative of the claimed invention, and it reads as follows:

12. A method for authenticating a first party at a second party, comprising:

(a) outputting a random number as a first challenge;

(b) receiving a second challenge and a first challenge response from said first party, said second challenge being a

count value, and said first challenge response being a result of performing a keyed cryptographic function (KCF) on said first challenge and said count value using a first key; and

(e) verifying said first party based on said first challenge, said second challenge, and said first challenge response.[1]

The prior art reference of record relied upon by the examiner in rejecting the appealed claims is:

Alfred Menezes et al., "Handbook of Applied Cryptography", CRC Press 1997, pp.397-404. (Menezes)

Claims 1-22 stand rejected under 35 U.S.C. § 103 as being unpatentable over Menezes.

Reference is made to the Examiner's Answer (Paper No. 12, mailed May 22, 2002) for the examiner's complete reasoning in support of the rejections, and to appellant's Brief (Paper No. 11 filed March 04, 2002) and Reply Brief (Paper No. 13, filed July 22, 2002) for the appellant's arguments thereagainst.

OPINION

As a preliminary matter, we note that appellant indicates on page 13 of the Brief that the claims are to be grouped together in eight groups. However, the appellant presented the same argument for claims 4, 9, 10, and 17 as for claims 13 and 16,

---

[1] Note that claim 12 and all claims dependent from claim 12 do not include steps (c) and (d) but jump directly from step (b) to step (e).

and, therefore, we regrouped the claims accordingly. The following groups remain:

GROUP I: Claims 12, 14, 15 and 18-20.

GROUP II: Claims 4, 9, 10, 13, 16 and 17.

GROUP III: Claims 1-3, 5, 6 and 11.

GROUP IV: Claims 7, 8, 21 and 22.

We have carefully considered the claims, the applied prior art reference, and the respective positions articulated by appellant and the examiner. As a consequence of our review, we will affirm the obviousness rejection of claims 1-6 and 9-20 and reverse the obviousness rejection of claims 7, 8, 21 and 22.

Group I: Claims 12, 14, 15 and 18-20.

Independent claim 12 recites in step (b) of the authenticating process that the second challenge received by the second party is a count value. The reference Menezes uses a random number as the second challenge instead of a count value (Menezes, page 402). The Examiner in rejecting the claim asserted that "pages 397-400 of Menezes et al. disclose interchangeability in authentication protocols of random numbers, such as r_A, with sequence numbers, such as the count value" (Final Rejection, page 7) and that "one of ordinary skill in the art would have known replay attacks were used to subvert

3

challenge-response authentication protocols, and therefore would have been familiar with choosing one of the three above options" (Answer, page 3) where by options he means one of random number, count value (otherwise known as sequence) and timestamp. In his Brief (page 15), the Appellant challenges the assertion that Menezes discloses such interchangeability and further submits that there is no requisite teaching or motivation presented for such a modification, since Examiner merely concluded that one could do so and not why one would do so. Thus, the focus is on the inadequacy of motivation presented as to why one would interchange the random number with a count value.

A careful look at Menezes discloses the following: time-variant parameters such as random numbers, sequences (i.e., count value) and timestamps are used in identification protocols to counteract replay and interleaving attacks. These protocols are in fact schemes put into place to reduce the vulnerability of the system so that when the communication line between two parties is monitored the response from one would not provide an adversary with useful information for subsequent identification (Menezes, page 397, paragraph 10.3.1). The time-variant parameters provide different securities, have strengths and weaknesses (random numbers are better at providing timeliness whereas count values are better at providing uniqueness), can be used in conjunction

as well as in combination with each other depending on the type of security sought (e.g., random numbers concatenated to timestamps or count values in a protocol guarantees that a pseudonumber will not be duplicated)(Menezes, pages 398-400). The protocol referred to in Menezes on page 402 follows the 9798-2 mechanism disclosed on page 401 with some modifications as shown. The 9798-2 mechanism provides in pertinent part that "in these mechanisms, the timestamp may be replaced by a sequence number" and "to avoid reliance on timestamps, the timestamp may be replaced by a random number, at the cost of an additional message". Thus, Menezes clearly discloses that timestamps, random numbers and sequences (i.e., count values) are interchangeable. Thus, in the SKID3 protocol the random number can be interchanged with a count value since a random number can be interchanged with a timestamp to reduce the amount of message sent (Menezes, page 401), and the timestamp can be interchanged with a count value to increase the uniqueness and security of the protocol (count values do not need time synchronization like timestamps do) (Menezes, page 398, 401).

The appellant also presented the argument (Brief, pages 16-17) that even if the second challenge (random number) were modified to include a count number in the SKID3 protocol, the resulting algorithm would not be the same as the one claimed

because it would omit message (1), i.e., it would omit the first
challenge sent and would omit performing a keyed cryptographic
function on both the count value and the first challenge as
required by claim 12. This argument, however, is not supported
because Menezes clearly shows protocol SKID3 as used for a one-
pass authentication where step (1) is required to complete the
authentication process (Menezes, page 402). Further, even if
using a count value instead of a random number eliminates one
message, that message is connected to the random number that was
interchanged with the count value, which in this case is the
random number present in step (2) and not the one present in step
(1). Menezes clearly discloses in step (2) on page 402 that the
keyed cryptographic function uses the first challenge.
Accordingly, we find appellant's arguments unpersuasive, and we
will sustain the rejection of claims 12, 14, 15, and 18-20.

Group II: Claims 4, 9, 10, 13, 16 and 17.

Appellant's argument (Brief, pages 17-19) focuses on the
fact that the Examiner failed to interpret the words "first key"
and a "second key" according to their plain meaning, namely, that
there are two separate keys. Also, Appellant asserts that the
Examiner failed to interpret the meaning of the claim altogether.
However, on page 401 Menezes clearly discloses that in

6

unidirectional communication, i.e., one-way protocols such as

SKID3, distinct keys K(AB) and K(BA) may be used instead of the

same key K. Thus, the key K used in step (2) can be different

than the key K used in step (3). Therefore, we will sustain the

rejection of claims 4, 9, 10, 13, 16, and 17.

Group III: Claims 1-3, 5, 6 and 11.

The representative claim in this group is claim 1 which has

the same limitation as claim 12, namely, that the second

challenge is a count value. As explained **supra**, this does not

differ from Menezes because although his protocol uses a random

number as the second challenge he discloses that count values can

be substituted for random numbers. Since the same argument was

presented (Brief, pages 21-22) for claim 12 as for claim 1, the

same response is pertinent here.

An additional argument was made (Brief, page 22) that

Menezes does not provide a teaching or suggestion to increment a

sequence number or count value in response to receiving the first

challenge. However, this argument is not persuasive because

Menezes clearly indicates that sequence numbers (count values),

when utilized in authentication protocols, inherently do just

that. Specifically, Menezes states that "the simplest policy is

that a sequence number starts at zero, is incremented

sequentially, and each successive message has a number one greater than the previous one received" (Menezes, page 399). Therefore, we will sustain the rejection of claims 1-3, 5, 6, and 11.

GROUP IV: Claims 7, 8, 21 and 22.

The Examiner stated on pages 5 and 6 of the Examiner's Answer that the rejection of these claims is overcome by appellant's arguments. Therefore, we reverse the rejection of claims 7, 8, 21 and 22.

CONCLUSION

The decision of the examiner rejecting claims 1-22 under 35 U.S.C. § 103 is affirmed as to claims 1-6 and 9-20 and reversed as to claims 7, 8, 21 and 22.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a).

AFFIRMED-IN-PART

KENNETH W. HAIRSTON
Administrative Patent Judge   )
)
)
)
ANITA PELLMAN GROSS   ) BOARD OF PATENT
Administrative Patent Judge   )   APPEALS
)   AND
) INTERFERENCES
)
)
)
HOWARD B. BLANKENSHIP   )
Administrative Patent Judge   )

AGP/RWK

9

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON VA 20195